Infoblox DNS Firewall
惡意軟體資料摘要服務概覽

Infoblox
CONTROL YOUR NETWORK

執行摘要

Infoblox 惡意軟體資料庫服務 (惡意軟體摘要) 會以接近即時的速度以最新的 DNS 惡意軟體相關資訊更新 Infoblox DNS 防火牆伺服器，以維持不間斷的有效性。惡意軟體摘要會利用來自 35 個以上的不同資源編譯七個不同的摘要，為不同規模、不同地理區域以及不同商業模式的組織 (包括國防與政府) 提供可調整的選擇。

惡意軟體摘要服務可封鎖因為 Bot、APT 以及其他類似威脅所感染的電腦，避免與其控制程式聯絡。它同時也可避免因為網路釣魚以及惡意病毒程式碼植入網站所造成的感染與資料遺失。

惡意軟體摘要包括網域名稱最新的 DNS 參考清單，以及在封鎖、重新導向或傳送 (全部透過一個記錄選項) 包括這些網域名稱的回覆時使用的相關原則。在擁有分散式 DNS 防火牆的環境中，管理員能夠讓惡意軟體資料摘要服務更新單一 DNS 防火牆伺服器 (會利用 Infoblox Grid™ 進行更新的內部分散)，或是讓資料摘要服務更新每個 DNS 防火牆。

快速概覽 - Infoblox DNS Firewall

DNS Firewall 是用於管理企業網路基礎結構的 Trinzic DDI (DNS、DHCP 以及 IP 位址管理) 解決方案的邏輯延伸。DNS 防火牆能夠阻止惡意軟體/僵屍網路利用 DNS 通訊協定找出並竊取資訊，並且將裝置轉變成「僵屍」網路電腦，幫助企業減少資料遺失與安全性攻擊。DNS 防火牆會透過從外部傳遞/傳送資訊的方式主動封鎖或重新導向 (或者略過並記錄) 惡意軟體。

DNS Firewall 會利用網路基礎結構中所有裝置的 Trinzic DDI 檢視以及 Trinzic Report 伺服器來報告有哪些裝置做出要求，進而讓 IT 能夠修復遭到感染的裝置。在重新導向原則中，登陸站台 / 圍牆花園 (Walled garden) 可以用來傳達消息，通知使用者關於請求站台的危險，以及如何聯絡 IT 進行安全修復措施。

DNS Firewall 在「深度防禦」策略中是重要的環節，因為它能夠針對公司所實施的傳統安全層 (例如防火牆、防毒軟體以及 IPS) 的不足進行補強。這些解決方案並不會為使用 DNS 來啟用通訊的所有各種通訊協定提供完整的範圍。

DNS Firewall 可阻止 DNS 查閱已經被識別為惡意的特定網域，也能夠封鎖存取已知被犯罪者所控制的 IP 位址或名稱伺服器上所託管的任何網域。它能夠防止電腦被重新導向至惡意站台，進而避免初始感染；也能夠封鎖已經避開其他偵測機制的受感染裝置，避免與其控制元件通訊或洩漏遭竊的資料。

在環境中加入 DNS Firewall 是在現有 Infoblox DNS 遞迴伺服器中增加一個簡單的授權附加元件。這個簡單的授權附加元件完全不需要加入新的裝置或重新建立網路基礎結構即可實施。

惡意軟體資料庫服務概覽

確保企業網路安全的挑戰就好比安全供應商與駭客以及惡意軟體/殭屍網路開發者在玩一場「貓捉老鼠」的遊戲。隨著保護網路的安全應用程式的演進，駭客以及惡意軟體/殭屍網路開發者也會修改其應用程式以便持續維持對企業基礎結構的攻擊。因此，任何安全解決方案必須持續改進，否則有可能成為安全配置中薄弱的環節。Infoblox 惡意軟體資料摘要服務的設計會根據各種惡意實體的 IP 位址、網域、URL、名稱伺服器以及更多內容讓 DNS 防火牆保持不斷更新。

可以利用來自全球超過 35 個不同公共與私人來源的資訊來開發惡意實體的多個資料摘要，這些是 DNS 防火牆在制定原則時不可缺少的一部份。來自不同來源的資訊會進行審查、資料關聯以及列入白名單的步驟，以便為要使用的 DNS 防火牆產生最新的惡意實體名單；如此可將主動錯誤訊息的機會減至最低。頻繁的更新程序意味著在清除受危害的伺服器時，也會將它們從清單中移除。對於客戶報告的假定主動錯誤訊息，Infoblox 支援團隊將會重新評估並且視需要採取糾正行動。

對於非跨國企業，且不可能有正當理由聯絡網際網路活動監管鬆散地區之電腦的組織而言，地理資料的增加將非常具有價值。結果為 Infoblox 資料庫服務會提供 DNS 防火牆所需要的資料，以便提供組織抵禦網路犯罪威脅所需要的保護。

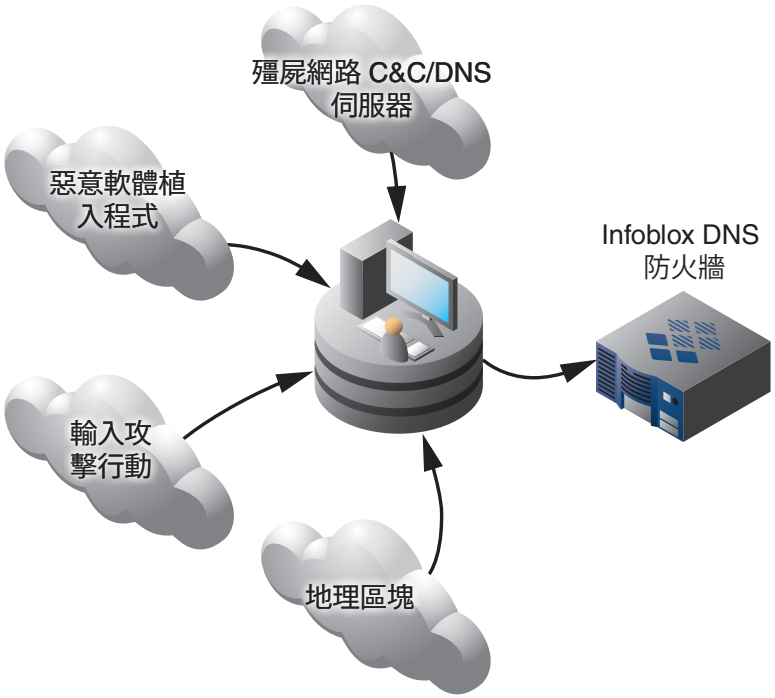
Infoblox DNS Firewall
惡意軟體資料摘要服務概覽

Infoblox
CONTROL YOUR NETWORK

cnc.rpz.infoblox.local	cnc-drivby.rpz.infoblox.local	malware.rpz.infoblox.local	malware-prc.rpz.infoblox.local	malware-ee.rpz.infoblox.local	malware-prc-ee.rpz.infoblox.local	malware-sanction.rpz.infoblox.local
Contains known command and control domains/IPs and dropboxes as well as name servers known to be used by malicious entities. This is a relatively small and focused list of the worst of the worst. In general it will not prevent initial infection but will prevent data exfiltration and identify infected devices that are looking for instructions.	Adds sites (IPs/domains/name servers) for known malware dropper sites & other places that can infect a computer that visits it. Includes networks & entire autonomous systems that are on the "Do not Route Or Peer" (DROP) list. This is an intermediate sized list that also blocks the worst infection vectors.	A comprehensive list of malware hosts/domains/name servers. In addition to the contents of the previous 2 feeds, contains including known active phishing sites and other threats. This is a comprehensive list of malicious locations on the internet.	Contains the malware data feed as well as the IP subnets, the ccTLD domain and name servers for the People's Republic of China.	Contains the malware data feed as well as the IP subnets, the ccTLD domains and name servers for countries in Eastern Europe that are major hosters of malware: Russia, Ukraine, Latvia, Moldova, and Romania.	Contains the malware data feed as well as the IP subnets, the ccTLD domains and name servers for the People's Republic of China and countries in Eastern Europe that are major hosters of malware: Russia, Ukraine, Latvia, Moldova, and Romania.	Contains the malware data feed as well as the IP subnets, the ccTLD domains and name servers for the countries on the OFAC Embargo and ITAR lists maintained by the US government. Currently the countries included are: Afghanistan, Belarus, Burma (Myanmar), China, Cote d'Ivoire, Cuba, Cyprus, Congo (Dem Rep), Eritrea, Haiti, Iran, Iraq, Lebanon, Liberia, Libya, North Korea, Sierra Leone, Somalia, Sri Lanka, Sudan, Syria, Venezuela, Vietnam, Yemen, Zimbabwe See http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx and http://pmddtc.state.gov/regulations_laws/itar_official.html

The geographic feeds provide protection against DNS Hijacks where popular domains are redirected malicious sites that are often located in other countries

圖 1：**Infoblox** 的 **DNS** 防火牆中可用的惡意軟體資料庫概覽。
由左至右移動 – 先前的惡意軟體資料庫是後續描述的資料庫服務（含）的子集。



在新的更新建立完成時，惡意軟體資料庫服務會將一個「NOTIFY (通知)」訊息傳送至 Infoblox DNS 防火牆伺服器。資料摘要服務接著會將大約數百個差異千位元組的遞增更新傳送至防火牆的埠 53。從惡意軟體資料庫服務到 DNS 防火牆伺服器的「NOTIFY (通知)」通訊一般為每 2 小時一次，但是如果來源提供的是變動快速的資訊，則頻率可以加快。

圖 2：用於惡意軟體資料庫服務 IP 資訊開發的來源基礎概覽。

Infoblox DNS Firewall
惡意軟體資料摘要服務概覽

Infoblox
CONTROL YOUR NETWORK

惡意軟體資料庫服務的散佈更新至 DNS 防火牆

許多企業使用分散式 DNS 防火牆架構來定位地理位置分散的大型網路，並且移除單一故障點。假設查詢請求會前往「區域性」DNS 遞迴伺服器，每個 DNS 防火牆必須持續更新，以便持續防範不斷改變的惡意軟體形態。管理員有 2 種組態選項可處理對於其分散式 DNS 防火牆的惡意軟體資料摘要服務更新。

選項 #1：RPZ 區域傳輸：惡意軟體資料庫服務更新是由屬於 Infoblox Grid 的 Infoblox DNS (防火牆) 同步處理成員所擷取。DNS 防火牆可以將惡意軟體資料庫資訊的 RPZ 區域傳輸執行至其他 DNS 防火牆伺服器。這個方法使得整個 DNS 防火牆的基礎結構能夠透過單一串流更新。

選項 #2：直接至每個遞迴伺服器：惡意軟體資料庫服務已設定為將更新直接傳送至每個客戶的遞迴 DNS 伺服器。

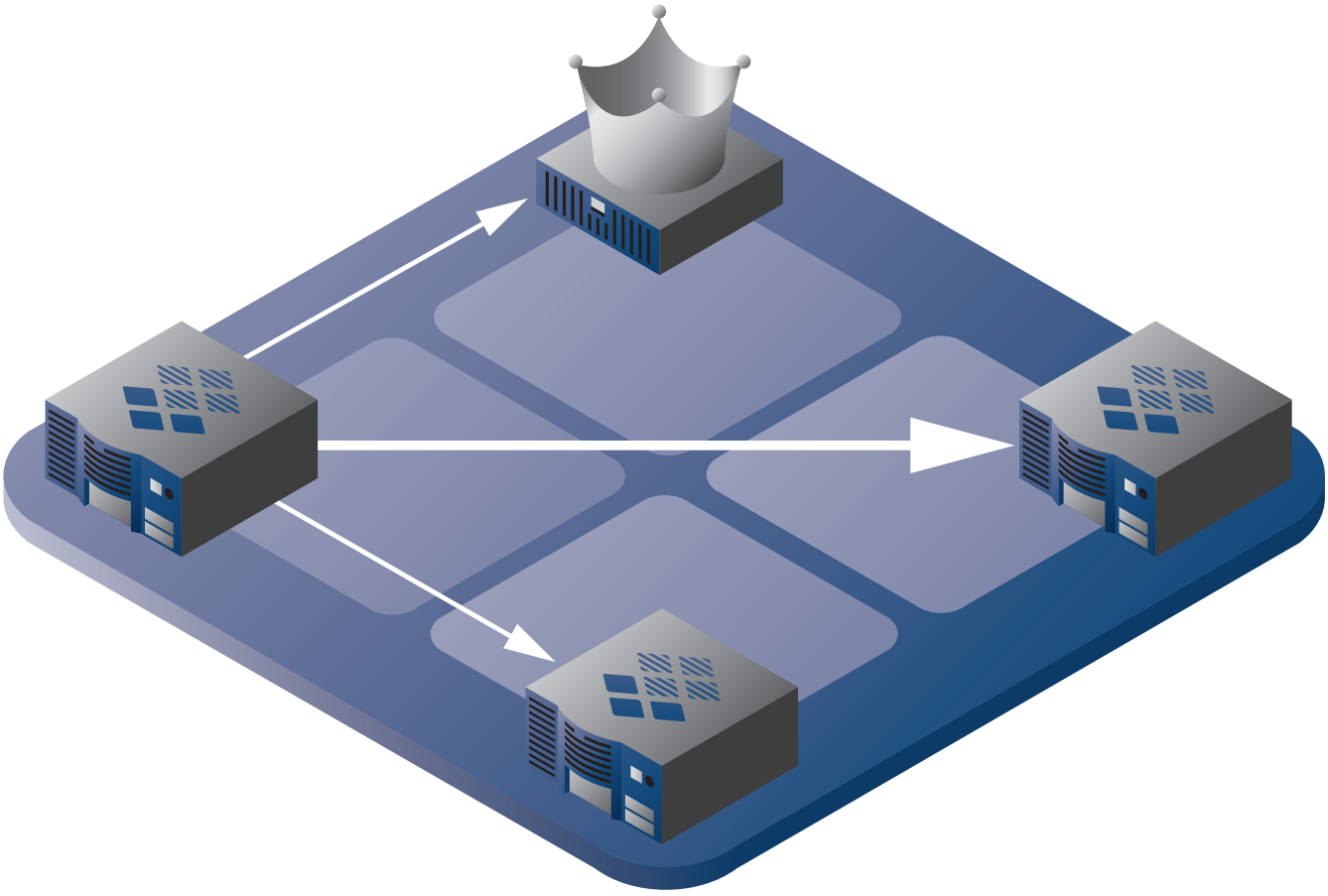


圖 3：單一惡意軟體資料摘要至管理內部散佈 DNS 防火牆同步處理成員。

Infoblox DNS Firewall
惡意軟體資料摘要服務概覽

Infoblox
CONTROL YOUR NETWORK

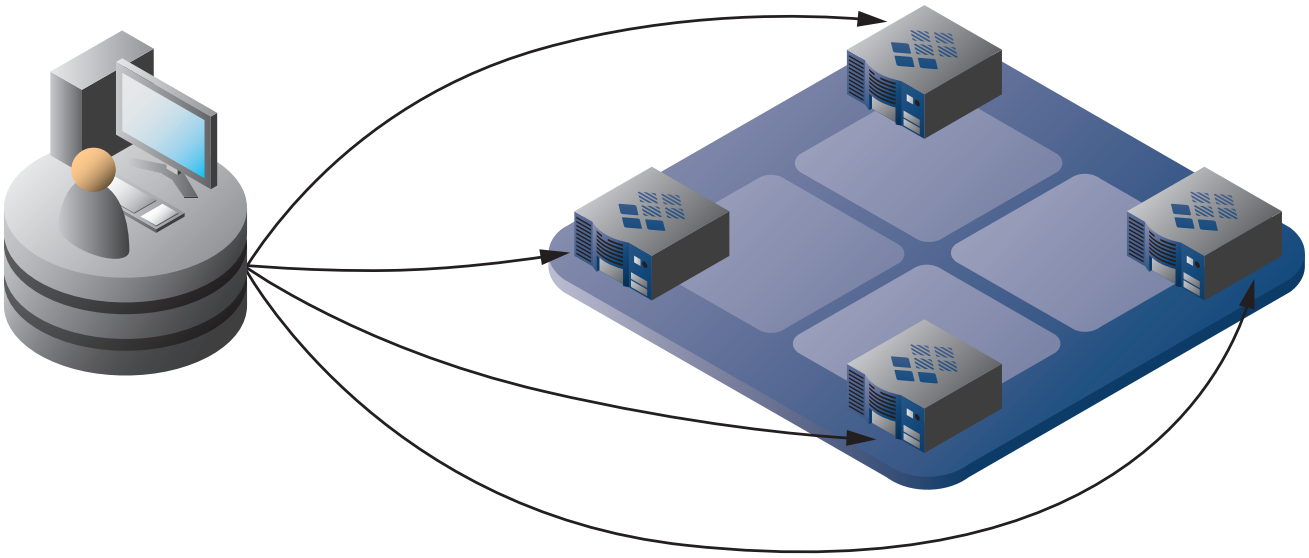


圖 4：惡意軟體資料摘要至每個遠端 DNS 防火牆。

摘要

Infoblox 中的惡意軟體資料庫服務是設計用來維持 DNS 防火牆 24 小時不間斷的有效性。惡意軟體資料庫服務提供 7 種不同的摘要類型 (來自全球 36 種不同的公共與私人來源) 以便提供彈性與保護，防範來自全球各地的惡意軟體與僵屍軟體。更新是透過區域傳輸安全地傳遞，而管理員能夠彈性地處理如何將資訊散佈至他們環境中各種不同的 DNS 防火牆。企業為減輕資料遺失的情況，會建立一些分層安全防禦。惡意軟體資料摘要服務能夠使得 DNS 防火牆在隔離這些防禦內部的 DNS「漏洞」上更具有效用。摘要也可以與多個內部與外部的信譽資料摘要合併。

Infoblox 產品保固與服務

標準硬體保固為期一年。系統軟體則提供90天保固，以使其符合公佈的規格。您亦可選購可延伸硬體和軟體保固的服務產品。建議您採用這些產品，以確保設備能取得最新的軟體增強功能，保持更新狀態，並確保系統的安全性和可用性。Infoblox 同時提供專業的服務和培訓課程。本文件中的資訊如有變更，恕不另行通知。Infoblox 公司對本文件中所出現的錯誤不承擔任何責任。

台灣分公司: 台北市信義區11047,松智路1號11樓1109室　電話:+886.2.8729.2154　sales-tw@infoblox.com　www.infoblox.com.cn | www.infoblox.com